UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,419	09/22/2003	John Purnell	113705	6513

25944   7590   08/10/2007
OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/665,419	PURNELL, JOHN
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 July 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-26</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-26</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

1.   This action is in reply to applicant's correspondence of 09 July 2007.

2.   Claims 1-26 are pending for examination.

3.   Claims 1-26 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on
> sale in this country, more than one year prior to the date of application for patent in the United States.

4.   Claims 1-5, 7, 9, 11-15, 17-19, 21-25 and 26 are rejected under 35 U.S.C. 102(b) as being

anticipated by McCoy et al, U.S. Patent No. 6,018,739.

5.   As per claim 1; "An identity management system to authenticate the identity of an

individual, comprising:

a vetting workstation

        to verify the identity of the individual and

        generate identification data *[Abstract, figures 1-3t and associated descriptions,*

whereas the distributed biometric identification system inclusive of a centralized (and

associated databases supporting the various workstations/client functions) server over a

wide area network (i.e., the Internet), and more particularly, the workstation utilized as

part of the subject (i.e., INS identification of individuals of targeted interest, inclusive of

(col. 1,lines 5-33) travelers, visitors, etc.,) biometric capture/administrative database

management (identity capture/verification) system, clearly encompasses the claimed

limitations as broadly interpreted by the examiner.];

an enrollment workstation

> to enroll the individual whose identity has been verified,
>
> to issue an identification token, and
>
> generate identification data *[Abstract, figures 1-3t and associated descriptions,*

whereas the distributed biometric identification system inclusive of a centralized (and

associated databases supporting the various workstations/client functions) server over a

wide area network (i.e., the Internet), and more particularly, the workstation utilized as

part of the subject (i.e., INS identification of individuals of targeted interest, inclusive of

(col. 1,lines 5-33) travelers, visitors, etc.,) biometric capture/administrative database

management (enrollment, whereas after enrolled, the system verified and issued

identification to the database constitutes a token data object) system, clearly

encompasses the claimed limitations as broadly interpreted by the examiner.]; and

a core system

> networked with
>
> > the vetting workstation and
> >
> > the enrollment workstation
>
> to provide
>
> > a central clearinghouse for the storage and
> >
> > exchange of identification data *[Abstract, figures 1-3t and associated*

descriptions, whereas the distributed biometric identification system inclusive of

clients, server(s), databases supporting the various workstations over a wide area

network (i.e., the Internet), and more particularly, the workstation utilized as part

of the subject biometric capture/administrative database management (client

requested database access to '...a central clearinghouse ...') system, clearly

encompasses the claimed limitations as broadly interpreted by the examiner.].".

And further as per claim 11, this claim is the method claim for the apparatus (system)

claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "An

identity management process for authenticating the identity of an individual, comprising:

pre-enrolling the individual in an identity management system by collecting personal

information submitted by the individual and storing the information in a database;

vetting the individual by authenticating the personal information through at least one

database of at least one of law enforcement, government and background checking

organizations;

enrolling the individual into the identity management system; comparing personal

information collected during pre-enrolling to data collected during enrolling;

vetting the individual by conducting at least a background check of the individual; and

issuing an identification token to the individual.".

And further as per claim 21, this claim is the embodied software claim for the apparatus

(system) claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection;

"A computer usable program embodied on a computer usable medium having computer readable

program code means, comprising:

  pre-enrolling an individual in the identity management system by recording personal

information submitted by the individual;

  enrolling the individual into the identity management system;

  vetting the individual by authenticating personal data through the query of a plurality of

databases including law enforcement, government and background checking organizations; and

  issuing an identity token to the individual.".

6.   Claim 2 *additionally recites* the limitations that; "The identity management system of

claim 1, further comprising

  a security check workstation

        to validate the identity of the individual at a facility using

              the identification token, and

        to record identification data, wherein

              the core system is networked with

                    a security check workstation.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of

the identification and administrative database management system (security check workstation

validation utilizing the identification token object and associated individual biometric fingerprint

capturing/comparison), clearly encompasses the claimed limitations as broadly interpreted by the

examiner.) suggest such limitations.

And further as per claim 15, this claim is the method claim for the apparatus (system)

claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; "The

identity management process of claim 11, further comprising

   conducting security checks at least one location using

      a security workstation

         by at least one of

            scanning the identity token of

               the individual,

            verifying biometric data of

               the individual and

            querying the core system for

               identity data.".

And further as per claim 25, this claim is the embodied software claim for the apparatus

(system) claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection;

"The computer program of claim 21, further comprising

   conducting security checks at various locations using

      one or more security workstations by at least one of

         scanning the identity token of

the individual,

verifying biometric data of

the individual and

querying the core system for

identity information.".

7.   Claim 3 *additionally recites* the limitations that; "The identity management system of

claim 1, further comprising

a check-in workstation for

checking-in individuals possessing the identification token,

wherein

the core system is networked with

the checking workstation.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of

the identification and administrative database management system (check-in workstation

utilizing the identification token object and associated individual biometric fingerprint

capturing/comparison), clearly encompasses the claimed limitations as broadly interpreted by the

examiner.) suggest such limitations.

And further as per claim 14, this claim is the method claim for the apparatus (system) claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The identity management process of claim 11, further comprising

checking-in the individual at a location

by at least one of

scanning the identification token of

the individual,

verifying biometric data of

the individual and

querying the core system for

identity data.".

And further as per claim 24, this claim is the embodied software claim for the apparatus (system) claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The computer program of claim 21, further comprising

checking-in the individual by at least one of

scanning the identity token of

the individual,

verifying biometric data of

the individual and

querying the core system for

identity information.".

8.   Claim 4 *additionally recites* the limitations that; "The identity management system

described in claim 3, wherein

   the check-in workstation is

      an automated kiosk.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of

the identification and administrative database management system (check-in workstation

utilizing the various remote (i.e., col. 5,lines 31-56) location configurations), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such

limitations.

9.   Claim 5 *additionally recites* the limitations that; "The identity management system

described in claim 1, further comprising

   a dispatch workstation

      to allow tracking of an individual with respect to the facility,

      to verify the individual's employee status, and

      to verify that the individual has a need to

         access certain areas of the facility,

   wherein

      the core system is electronically connected with

the dispatch workstation.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of

the identification and administrative database management system (dispatch workstation

inclusive of validation of individual access rights with respect to a facility, INS related employee

status aspects, etc.,), clearly encompasses the claimed limitations as broadly interpreted by the

examiner.) suggest such limitations.

10.   Claim 7 *additionally recites* the limitations that; "The identity management system

described in claim 1, wherein   '

        the core system is electronically connected with

                the vetting workstation and

                the enrollment workstation

        using

                a secure connection.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet, whereas inclusive of SSL, IPSec (the WEB secure

communications aspects), etc.,), clearly encompasses the claimed limitations as broadly

interpreted by the examiner.) suggest such limitations.

11.   Claim 9 *additionally recites* the limitations that; "The identity management system

described in claim 5, wherein

 the core system is networked with

  the dispatch workstation

using

  a secure connection.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet, whereas inclusive of SSL, IPSec (the WEB secure

communications aspects), etc.,), clearly encompasses the claimed limitations as broadly

interpreted by the examiner.) suggest such limitations.

12.   Claim 12 *additionally recites* the limitations that; "The identity management process of

claim 11, wherein

 pre-enrolling employs at least one of

  the Internet,

  mail service, and

  personal appearance.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet, whereas inclusive of SSL, IPSec (the WEB secure

communications aspects), etc.,) and personal pre-enrolling via client workstations, clearly

encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such

limitations.

And further as per claim 22, this claim is the embodied software claim for the method

claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection; "The

computer program of claim 21, wherein

> pre-enrolling employs at least one of

>> the Internet,

>> mail service, and

>> personal appearance.".

13.   Claim 13 *additionally recites* the limitations that; "The identity management process of

claim 11, further comprising

> submitting biometric data for

>> identification purposes.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network, and personal pre-enrolling via client workstations submission of biometric

data, clearly encompasses the claimed limitations as broadly interpreted by the examiner.)

suggest such limitations.

And further as per claim 23, this claim is the embodied software claim for the method

claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection; "The

computer program of claim 21, further comprising

submitting biometric data.".

14.   Claim 17 *additionally recites* the limitations that; "The identity management process of

claim 14, wherein

checking-in includes

obtaining the identity information queried from the core system

that includes at least one of

a facial image,

an iris scan,

hand geometry,

a fingerprint, and

the like.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network, and checking-in via client workstations submission of biometric (i.e.,

fingerprint, facial) data, clearly encompasses the claimed limitations as broadly interpreted by

the examiner.) suggest such limitations.

15.   Claim 18 *additionally recites* the limitations that; "The identity management process of

claim 15, wherein

    conducting security checks includes

        obtaining identity information queried from the core system

            that includes at least one of

                a facial image,

                an iris scan,

                hand geometry,

                a fingerprint, and

                the like.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network, and conducting security checks via client workstations submission of

biometric (i.e., fingerprint, facial) data, clearly encompasses the claimed limitations as broadly

interpreted by the examiner.) suggest such limitations.

16.   Claim 19 *additionally recites* the limitations that; "The identity management process of

claim 16, wherein

    identity verification includes

        obtaining identity information queried from the core system

            includes at least one of

                a facial image,

an iris scan,

hand geometry,

a fingerprint, and

the like.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network, and identity verification via client workstations submission of biometric

(i.e., fingerprint, facial) data, clearly encompasses the claimed limitations as broadly interpreted

by the examiner.) suggest such limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

17.   Claims 6, 8, 10, 16, 20 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable

over McCoy et al, U.S. Patent No. 6,018,739, and further in view of below.

It is noted that McCoy et al does not disclose the distributed biometric identification

system utilized in the transportation environment per se. However, the examiner asserts that it

would have been obvious to one ordinary skill in the art at the time the invention was made for

the INS to use the McCoy system as part of a transportation access control mechanism, since

such control of access to transportation means/boarding, etc., by individuals under identification

by the INS would be obvious. A recitation directed to the manner in which a claimed apparatus is

intended to be used does not distinguish the claimed apparatus from the prior art if prior art has

the capability to do so (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987).

18.   Claim 6 *additionally recites* the limitations that; "The identity management system

described in claim 1, further comprising

    a boarding workstation

        to authorize an individual

            to board a means of transportation based on

                verification of the identity and

                travel information regarding the individual,

      wherein

            the core system is electronically connected to

                the boarding workstation.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of

the identification and administrative database management system (boarding workstation

inclusive of authorization of individual access rights with respect to boarding, etc.,), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such

limitations.

And further as per claim 16, this claim is the method claim for the apparatus (system)

claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; "The

identity management process of claim 11, further comprising

    identity verification

        prior to boarding a means of transportation

           by at least one of

                scanning the identification token of

                    the individual,

                verifying biometric data of

                    the individual and

                querying the core system for

                    identity and

                    travel information.".

And further as per claim 26, this claim is the embodied software claim for the apparatus

(system) claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection;

"The computer program of claim 21, further comprising

    boarding onto the means of transportation by

        at least one of

           scanning the identity token of

              the individual,

           verifying biometric data of

the individual and

querying the core system for

identity and

travel information.".

19.   Claim 8 *additionally recites* the limitations that; "The identity management system described in claim 6, wherein

the core system is networked with

the check-in workstation and

the boarding workstation

using

a secure connection.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the distributed biometric identification system inclusive of various workstations/client functions over a wide area network (i.e., the Internet, whereas inclusive of SSL, IPSec (the WEB secure communications aspects), etc.,), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

20.   Claim 10 *additionally recites* the limitations that; "The identity management system described in claim 3, further comprising

a boarding workstation

to authorize an individual

to board a means of transportation based on

verification of the identity and

travel information regarding the individual,

wherein

the core system is electronically connected to

the boarding workstation.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the

distributed biometric identification system inclusive of various workstations/client functions over

a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of

the identification and administrative database management system (boarding workstation

inclusive of authorization of individual access rights with respect to boarding, etc.,), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such

limitations.

21.   Claim 20 *additionally recites* the limitations that; "The identity management process of

claim 11, wherein

pre-enrolling,

enrolling and

vetting

are performed in accord with

an access control system of

a transportation facility.".

The teachings of McCoy et al (Abstract, figures 1-3t and associated descriptions, whereas the distributed biometric identification system inclusive of various workstations/client functions over a wide area network (i.e., the Internet), and more particularly, the workstation utilized as part of the identification and administrative database management system (boarding workstation inclusive of authorization of individual access rights with respect to boarding, etc.,), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

Response to Amendment

22.   As per applicant's argument concerning the lack of teaching by McCoy et al of an identification token insofar as a smart card or physical token per se is defined in the specification (i.e., paragraph 0010), and further, of a vetting of the individual insofar as a background check, etc., is concerned, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

At the very least, the McCoy et al security objects created in the biometric assessment and database storage of said objects throughout the personnel identification system client/server network components, clearly encompasses the identification token aspects of the claim 1 limitations insofar as the specification gives an example versus an actual definition of an identification token, thereby necessitating a broad interpretation of the term to encompass anything from a password (i.e., virtual identification token) up to a physical token (i.e., smart card, etc.,). Also, the "... vetting ... background ..." aspects of the claim are clearly covered by the fact that the McCoy et al biometric assessment and database storage of individual collected

information is in itself a collection of background information, as broadly interpreted by the

examiner, as per the claim language, and would therefore be applicable in the rejection, such that

the rejection support references collectively encompass the said claim limitations in their

entirety.

23.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Conclusion

24.   Any inquiry concerning this communication or earlier communications from examiner

should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose

unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The

examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the

organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. For more information for

unpublished applications is available through Private PAIR only. For more information about the

PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Patent Examiner

8, 8, 0 7